IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants:	Antonio Lain and Viacheslav Borisov		
Assignee:	Hewlett-Packard Development Company, L.P.		
Title:	Cryptographic Key Update Management Method and Apparatus		
Serial No.:	10/814,608	Confirmation No.	5425
Docket No.:	200310005-2	Filing Date:	March 30, 2004
Examiner:	Bryan F. Wright	Group Art Unit:	2431

April 6, 2009

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF UNDER 37 C.F.R. § 1.191

Dear Sir:

Appellants submit this Appeal Brief pursuant to the Notice of Appeal filed in the above-identified patent application on February 5, 2009. Payment of the required fee for this Appeal Brief is authorized in an accompanying document. No extension of time is believed necessary since April 5, 2009 fell on a Sunday. However, if an extension is required, the Commissioner is hereby authorized to treat this document as containing a request for the required extension of time for filing this appeal brief and is further authorized to charge any additional fee which may be required to deposit account No. 08-2025.

I. REAL PARTY IN INTEREST

The real party in interest is the assignee, Hewlett-Packard Development Company, L.P., as named in the caption above.

II. RELATED APPEALS AND INTERFERENCES

Based on information and belief, there are no prior or pending appeals, interferences or judicial proceedings known to Appellant, the Appellant's legal representative, or assignee which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

III. STATUS OF CLAIMS

Claims 1-21 are pending in this case and all stand rejected.

IV. STATUS OF AMENDMENTS

There are no unentered amendments in this case. No amendments were filed subsequent to the final rejection dated November 5, 2008.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The claimed subject matter is generally related to secure communications among members of a group using a logical key hierarchy ("LKH") such as LKH 120 in Fig. 2 of Appellants' specification. Such a hierarchy is established for clients that are associated with respective leaf keys of the hierarchy. Each client knows its leaf key and all the other keys in the path from that leaf key to the root key of the LKH. The root key of the LKH is a group key and can be used to send a secure message to all the clients in the group. As described on page 1 of Appellants' specification, the keys need to be updated to maintain security when a client joins or leaves the group. Updating conventionally involves sending update records to the current clients. The subject matter on appeal addresses the problem of how to update a client that has been offline and therefore has missed a number of update records. The claimed solution particularly employs an entity (KHT cache 20 in Fig. 1 of Appellants' specification) that receives all update records and consolidates the update records into a "key history tree" (KHT) that a re-connecting client can use to update the set of keys that that client is authorized to have. This key history tree (KHT) is not the same as the logical key hierarchy (LKH).

Independent claim 1 specifically recites "Apparatus for consolidating key updates." An example of such apparatus is KHT cache 20 of Fig. 1, which is introduced in the paragraph beginning at page 4, line 30. As recited in claim 1, each record that provides a key update includes "an encrypted key corresponding to a node of a key hierarchy and encrypted using a key which is a descendant of that node, hierarchy-node information for both the encrypted and encrypting keys, and key-version information for at least the encrypted key." Such records are illustrated by update records 18 in Fig. 1. (See also page 7, lines 16-23 and page 8, lines 4-13 for a description of record content.) Claim 1 further recites that the apparatus includes "a communications interface for receiving said records and a manager," e.g., communication interface 21 and manager 22 of Fig. 1. For the manager, claim 1 recites, "maintaining, on the basis of the received records, a key tree," which corresponds in an illustrated embodiment to

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

key history tree 24 of Fig. 1. "A key tree with nodes corresponding to nodes in said hierarchy" is described beginning at page 9, line 16. Claim 1 finally recites "the manager being arranged to store in association with each tree node, for each encrypting key used in respect of the encrypted key associated with the node, the most up-to-date version of the encrypted key and its version information with any earlier versions being discarded." An example of the maintenance of a key history tree containing encrypted keys is illustrated in Fig. 3, and description of operation of a manager to store and overwrite nodes of a key history tree can be found beginning at page 9, line 31. More particularly, storing up-to-date encrypted keys at nodes is described, for example, in the paragraph beginning at page 10, line 9. Discarding earlier versions is described, for example, in page 10, lines 28-32.

Independent claim 13 recites, "A method of consolidating key updates provided in records each comprising an encrypted key corresponding to a node of a key hierarchy and encrypted using a key which is a descendant of that node, hierarchy-node information for both the encrypted and encrypting keys, and key-version information for at least the encrypted key." Key updates and their contents are described in page 7, lines 16-23 and page 8, lines 4-13." Claim 13 further recites, "the method comprising ... maintaining, on the basis of said records, a key tree with nodes corresponding to nodes in said hierarchy." An example of the maintenance of a key history tree is illustrated in Fig. 3, and description of operation of a manager for a key history tree can be found beginning at page 9, line 31. Claim 13 finally recites, "this tree-maintenance step comprising ... storing in association with each tree node, for each encrypting key used in respect of the encrypted key associated with the node, the most up-to-date version of the encrypted key and its version information with any earlier versions being discarded." Storing up-to-date encrypted keys at nodes is described, for example, in the paragraph beginning at page 10, line 9. Discarding earlier versions is described, for example, in page 10, lines 28-32.

Claim 21 recites, "A method of providing key updates to members of a group, comprising the steps of: managing a key hierarchy in dependence on the addition and/or removal of members to said group." Managing a key hierarchy, e.g., LKH, is illustrated in Fig. 2 and described beginning at page 5, line 20 The step of "outputting, as notification of the changes made to the key hierarchy, records that each comprise an encrypted key corresponding to a node of the key hierarchy and encrypted using a key which is a descendant of that node, and hierarchy-node and key-version information for both the encrypted and encrypting keys" is described, for example, in page 8, lines 3-13. Claim 21 further recites,

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH (530) 621-4545
FX (530) 621-4543

"consolidating said records according to the method of claim 13." The method of claim 13 is summarized above with references to page and line numbers in the specification. Claim 21 finally recites, "providing said key tree, or a subset of it, to members of said group whereby to enable these members to recover the current root key of the key hierarchy at least within a target failure margin." See the paragraph beginning at page 9, line 7.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The following issues are presented to the Board of Patent Appeals and Interferences for decision:

A. Whether Claims 1-5, 8-17, 20, and 21 are anticipated under 35 U.S.C. 102(b) by the paper of Chung Kei Wong, entitled "Secure Group Communications Using Key Graphs," IEEE/ACM Transactions on Networking, Vol. 8, No. 1, Feb 2000 (hereinafter Wong).

B. Whether Claims 6, 7, 18, and 19 are unpatentable under 35 U.S.C. 103(a) over Wong in view of U.S. Patent No. 6,606,706 (hereinafter Li).

VII. ARGUMENT

A. Claims 1-5, 8-17, 20, and 21 are patentable under 35 U.S.C. 102(b) over Wong.

Claims 1-5 and 8-12

Independent claim 1 distinguishes over Wong at least by reciting, "Apparatus for consolidating key updates … comprising … a manager for maintaining, on the basis of the received records, a key tree with nodes corresponding to nodes in said hierarchy." Wong is directed to secure communications using related or hierarchical keys, but the only key tree that Wong discloses is the logical key hierarchy. In Wong, the trusted server that maintains the logical key hierarchy also generates the key updates or rekey messages. Wong fails to disclose or suggest a key tree with nodes corresponding to the hierarchy and maintained based on **received** records of the type recited in claim 1.

In regard to the manager recited in claim 1, the Examiner cites the trusted key server (i.e., server s) of Wong. Wong at page 19, left column, lines 25-30 describes, "After each join or leave, a new secure group is formed. Server s has to update the group's key graph by

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

replacing the keys of some existing k-nodes, deleting some k-nodes (in the case of a leave), and adding some k-nodes (in the case of a join). It then securely sends rekey messages containing new group/subgroup keys to users of the new secure group." The trusted key server s thus maintains the logical key hierarchy, which Wong calls the "group key graph." Further, the server s generates the key update messages (called "rekey messages" in Wong) for updating the users. Wong fails to suggest that the server s maintains a key tree separate from the hierarchy or maintaining a key tree based on received records.

Wong further fails to suggest consolidating key updates as recited in claim 1. Clearly, the trusted key server s of Wong generates and sends the key updates based on the group's key graph, and Wong fails to suggest a need to consolidate updates. Each user u in Wong is only interested in the keys lying in the path from an associated leaf node of the group key graph and the root of the graph. No user needs to construct a key tree, and Wong does not disclose the construction of such a graph by a user.

Claim 1 further distinguishes over Wong by reciting, "the manager being arranged to store in association with each tree node, for each encrypting key used in respect of the encrypted key associated with the node, the most up-to-date version of the encrypted key and its version information with any earlier versions being discarded." The rekey messages of Wong include keys encrypted by other keys. (See, for example, the first paragraph in the right column on page 20 of Wong.) But, Wong fails to disclose or suggest maintaining a key tree and storing in association with the nodes of this tree, **encrypted** keys such as received in rekey messages. The server s of Wong stores un-encrypted keys that are encrypted for rekey messages and decrypted by users u.

In accordance with an aspect of Appellants' invention, a key tree (e.g., KHT) is built from the update records, and stored in association with each node are one or more encryptions of the corresponding key of the key hierarchy. Encrypted keys are maintained for security and because valid reconnecting clients already have the keys necessary for decryption. (There can be "one or more" encrypted keys because there can be respective encryptions for descendent nodes.) Thus, while the LHK or the hierarchy disclosed by Wong is a hierarchy of unencrypted keys, the KHT is a hierarchy of encrypted keys. Wong does not suggest such a hierarchy of encrypted keys, and Wong does not address the problem of clients (or users) missing key updates (or missing rekey messages). Claim 1 is thus patentable over Wong.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

Claims 2-5 and 8-12 depend from clam 1 and are patentable over Wong for at least the same reasons that claim 1 is patentable over Wong.

Claims 13-17, 20, and 21

Independent claim 13 distinguishes over Wong at least by reciting, "A method of consolidating key updates … comprising a step of maintaining, on the basis of said records, a key tree with nodes corresponding to nodes in said hierarchy." As noted above, Wong fails to disclose or suggest "consolidating key updates" or "maintaining, on the basis of said records a key structure." In particular, Wong describes a server s that generates rekey messages and users u that decrypt and use rekey messages, but Wong fails to suggest consolidating the rekey messages. Further, Wong only describes server s maintaining a key tree, and server s generates the rekey messages from the group's key graph, rather than maintaining a key tree based on records of the type recited in claim 13.

Claim 13 further distinguishes over Wong by reciting, "storing in association with each tree node, for each encrypting key used in respect of the encrypted key associated with the node, the most up-to-date version of the encrypted key and its version information with any earlier versions being discarded." As noted above, the only tree structure described by Wong contains un-encrypted keys. Accordingly, claim 13 is patentable over Wong.

Claims 14-20 depend from claim 13 and are patentable over Wong for at least the same reasons that claim 13 is patentable over Wong.

Claim 21 recites "consolidating said records according to the method of claim 13" and is thus also patentable over Wong for at least the same reasons that claim 13 is patentable over Wong.

B. Claims 6, 7, 18, and 19 are patentable under 35 U.S.C. 103(a) over Wong in view of Li.

Claims 6 and 7

Claims 6 and 7 depend from claim 1, which is patentable over Wong for the reasons given above. In particular, Wong fails to disclose or suggest consolidating received update messages and maintaining a key tree of encrypted keys. Li is directed to multicast networks that are split into multiple security domains. The Examiner cites Li as teaching limitations of claims 6 and 7 that are not found in base claim 1. See the Final Office Action beginning on page 13, line 15. Although Appellants' disagree with the Examiner's interpretation of Li, that issue is not relevant in this Appeal because Appellants are not separately arguing the reasons for patentability of these dependent claims. Appellants instead note that Li, whether

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

considered alone or in combination with Wong, fails to disclose or suggest consolidating received update messages and maintaining a key tree of encrypted keys. Accordingly, claim 1 and claims 6 and 7, which depend from claim 1, are patentable over the combination of Wong and Li.

Claims 18 and 19

Claims 18 and 19 depend from claim 13, which is patentable over Wong for the reasons given above. Again, Wong fails to disclose or suggest consolidating received update messages and maintaining a key tree of encrypted keys. Combining Li with Wong still fails to disclose or suggest the method of claim 13. Accordingly, claim 13 and claims 18 and 19, which depend from claim 13, are patentable over the combination of Wong and Li.

For the above reasons, Appellants respectfully submit that pending claims 1-21 are allowable. Accordingly, Appellants submit the present rejection is unfounded and request that the rejections of claims 1-21 be reversed.

Please contact the undersigned attorney at (530) 621-4545 if there are any questions concerning this Appeal Brief or the application generally.

:

Respectfully submitted,

/David Millers 37396/

David Millers
Reg. No. 37,396

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH (530) 621-4545
FX (530) 621-4543

VIII. CLAIMS APPENDIX

Claims 1-21, which are the claims involved in this appeal, are copied below.

1. Apparatus for consolidating key updates provided in records that each comprise an encrypted key corresponding to a node of a key hierarchy and encrypted using a key which is a descendant of that node, hierarchy-node information for both the encrypted and encrypting keys, and key-version information for at least the encrypted key; the apparatus comprising a communications interface for receiving said records, and a manager for maintaining, on the basis of the received records, a key tree with nodes corresponding to nodes in said hierarchy, the manager being arranged to store in association with each tree node, for each encrypting key used in respect of the encrypted key associated with the node, the most up-to-date version of the encrypted key and its version information with any earlier versions being discarded.

2. Apparatus according to claim 1, wherein the manager is arranged to store each said most up-to-date version of a said encrypted key by storing the record containing the latter with any previously-stored record that is thereby superseded being discarded.

3. Apparatus according to claim 1, wherein the manager is arranged to store in association with each tree node, along with the most up-to-date version of the corresponding encrypted key stored for each encrypting key used in respect of that encrypted key, version information for the encrypting key used to encrypt said most up-to-date version of the encrypted key, this version information being included in the record providing said most up-to-date version of the encrypted key.

4. Apparatus according to claim 3, wherein the manager is arranged to replace the version of the encrypted key stored in association with a tree node for a particular encrypting key, with any subsequently received later version of that key provided the latter has been encrypted with a version of the encrypting key that is the same or later than the version used for encrypting the existing stored encrypted key.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

5. Apparatus according to claim 1, further comprising a working-set generator for processing the key tree to generate a subset of the tree enabling, at least within a target failure rate, all clients associated with the key hierarchy to recover the current root key of the latter.

6. Apparatus according to claim 5, wherein the working set generator comprises control means for receiving feedback on the current root-key recovery failure rate and for controlling the size of said subset to approach the actual failure rate to said target failure rate.

7. Apparatus according to claim 6, wherein the working set generator further comprises means for determining the likelihood of a tree node being required to enable recovery the current root key, these means being based on at least one of the age of the node, or of an encrypted key associated with it, and an estimate of the number of possible clients that will need the node.

8. Apparatus according to claim 1, wherein the manager is arranged to maintain said tree only in respect of keys corresponding to the nodes of a predetermined sub-hierarchy of said hierarchy and keys for the path from the head of this sub-hierarchy that terminates at the root of the hierarchy.

9. A system comprising apparatus according to claim 1, and a key-hierarchy manager for managing said key hierarchy in dependence on the addition and/or removal of members to a group, the key-hierarchy manager being arranged to output said records both to currently available members of said group and to said apparatus as notification of the changes made by the key-hierarchy manager to the key hierarchy, said apparatus being arranged to provide said key tree, or a subset of it, to members of said group who subsequently become available as a consolidated notification of the changes made by the key-hierarchy manager to the key hierarchy whereby to enable these members to recover the current root key of the key hierarchy at least within a target failure margin.

10. A system comprising apparatus according to claim 1, and a key-hierarchy manager for managing said key hierarchy in dependence on the addition and/or removal of members to a group, the key-hierarchy manager being arranged to output said records to said apparatus, said apparatus being arranged to provide said key tree, or a subset of it, to members of said group as a consolidated notification of the changes made by the key-hierarchy

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

manager to the key hierarchy whereby to enable these members to recover the current root key of the key hierarchy at least within a target failure margin.

11. A system according to claim 10, wherein the key-hierarchy manager and said apparatus form part of an anonymous group content distribution arrangement; the key tree, or a subset of it, being sent to group members in association with content encrypted with a key that is one of:

- the key-hierarchy root key, and
- a key encrypted using the key-hierarchy root key and provided in encrypted form along with the encrypted content.

12. A system comprising multiple apparatuses according to claim 1, and a key-hierarchy manager for managing said key hierarchy in dependence on the addition and/or removal of members to a group and for outputting key update records reflecting changes made to the key hierarchy; the apparatuses being configured in a multiple-level hierarchical arrangement comprising a first-level apparatus arranged to receive the records output by the key-hierarchy manager, and one or more lower levels of apparatuses each arranged to receive the key tree, or a subset of it, produced by a said apparatus at the next level up, the apparatuses at the lowest level of the hierarchical arrangement each being arranged to provide its key tree, or a subset of it, to a respective sub-group of members of said group; the apparatuses at each level of said hierarchical arrangement, other than said first level, each being arranged to maintain its said tree only in respect of keys corresponding to the nodes of a respective predetermined sub-hierarchy of said key hierarchy and keys for the path from the head of this sub-hierarchy that terminates at the root of the key hierarchy.

13. A method of consolidating key updates provided in records each comprising an encrypted key corresponding to a node of a key hierarchy and encrypted using a key which is a descendant of that node, hierarchy-node information for both the encrypted and encrypting keys, and key-version information for at least the encrypted key; the method comprising a step of maintaining, on the basis of said records, a key tree with nodes corresponding to nodes in said hierarchy, this tree-maintenance step comprising a sub-step of storing in association with each tree node, for each encrypting key used in respect of the encrypted key associated

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH (530) 621-4545
FX (530) 621-4543

with the node, the most up-to-date version of the encrypted key and its version information with any earlier versions being discarded.

14. A method according to claim 13, wherein in said sub-step each said most up-to-date version of a said encrypted key is stored by storing the record containing the latter with any previously-stored record that is thereby superseded being discarded.

15. A method according to claim 13, wherein in said sub-step the version information of the encrypting key used to encrypt said most up-to-date version of the encrypted key is stored with the latter.

16. A method according to claim 13, wherein in said sub-step the version of the encrypted key stored in association with a tree node for a particular encrypting key, is replaced with any subsequently received later version of that key provided the latter has been encrypted with a version of the encrypting key that is the same or later than the version used for encrypting the existing stored encrypted key.

17. A method according to claim 13, further comprising the further step of processing the key tree to generate a subset of the tree enabling, at least within a target failure rate, all clients associated with the key hierarchy to recover the current root key of the hierarchy.

18. A method according to claim 17, wherein the further step comprises receiving feedback on the current root-key recovery failure rate and controlling the size of said subset to approach the actual failure rate to said target failure rate.

19. A method according to claim 18, wherein said further step further comprises determining the likelihood of a tree node being required to enable recovery the current root key, this determination being based on at least one of the age of the node, or of an encrypted key associated with it, and an estimate of the number of possible clients that will need the node.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH (530) 621-4545
FX (530) 621-4543

20. A method according to claim 13, wherein said tree is maintained only in respect of keys corresponding to the nodes of a predetermined sub-hierarchy of said key hierarchy

and keys for the path from the head of this sub-hierarchy that terminates at the root of the hierarchy.

21. A method of providing key updates to members of a group, comprising the steps of:

managing a key hierarchy in dependence on the addition and/or removal of members to said group and outputting, as notification of the changes made to the key hierarchy, records that each comprise an encrypted key corresponding to a node of the key hierarchy and encrypted using a key which is a descendant of that node, and hierarchy-node and key-version information for both the encrypted and encrypting keys; and

consolidating said records according to the method of claim 13 and providing said key tree, or a subset of it, to members of said group whereby to enable these members to recover the current root key of the key hierarchy at least within a target failure margin.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

IX. EVIDENCE APPENDIX

There is no evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 or any other evidence entered by the examiner that Appellant is relying upon in this appeal.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

X. RELATED PROCEEDINGS APPENDIX

No decisions rendered by a court or the Board of Patent Appeals and Interferences are being submitted.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543